SECURITY FRAMEWORK FOR WIRELESS SENSOR NETWORKS

SYNOPSIS

DOCTOR OF PHILOSOPHY
IN
COMPUTER SCIENCE AND ENGINEERING

By
ROHIT VAID
(11118950)
Under the Supervision of

Dr. VIJAY KUMAR
(Supervisor)
Professor
Computer Science & Engineering Department
M. M. Engineering College, Mullana
Ambala

M. M. University, Mullana, Ambala
December 2012

Contents

1. Wireless sensor network overview
2. Security requirements in WSN
3. Literature review
4. Research objective
5. Works to be carried out
6. References

SECURITY FRAMEWORK FOR WIRELESS SENSOR NETWORKS

The increasing ability of wireless communication has attracted a great attention towards wireless sensor networks (WSNs) in recent years. WSNs are self-organized, autonomous systems consisting of number of battery powered sensors nodes responsible for transmitting the real-time sensed data in specific monitoring environment to the base station where it can be further processed and analyzed. However, chances are more that WSNs are easily compromised due to wireless communication. Existing solutions dedicated to wired networks are not suited in WSNs due to limited hardware resource and computing constraints. So we need a simple model that would enable fully functional security in WSNs.

1. WIRELESS SENSOR NETWORK

A wireless sensor network consist of large number of wireless devices able to take environmental measurements (temperature, light, sound, and humidity).The network consist of large number of sensor nodes which are small in size, equipped with embedded processors, sensors, radio transmitter and receiver. These sensor nodes have not only data processing capabilities but also sensing and communicating capability.

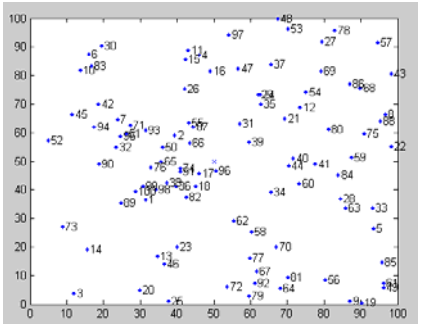

Figure 1: Randomly deployed sensor nodes

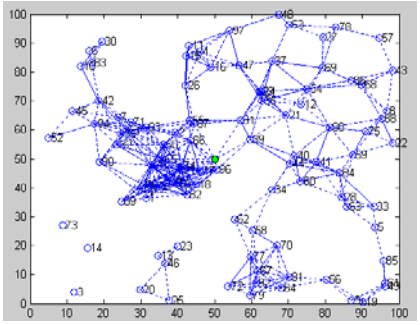

Figure 2: Neighboring graph created by randomly deployed sensor nodes

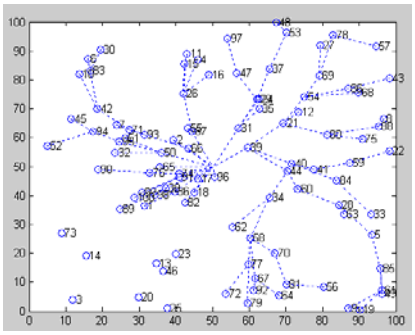

Figure 3: Shortest path graph to base station in WSNs

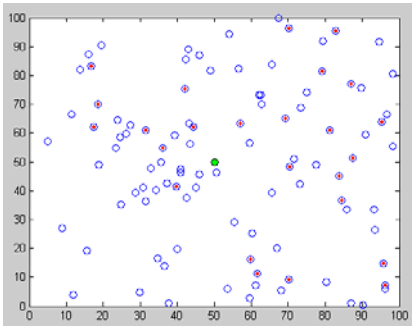

Figure 4: WSN with dead node

Figure 1 show a simple wireless sensor networks which is randomly deployed. In Figure 2 the neighboring graph created by each sensor according to its range is shown with the help of a link where a sensor will communicate directly in a single hope. Figure 3 show a shortest path of each sensor to base station where a base station is shown by ID 101. The scenario when the node are dead due to loss of energy or by some other reason are shown in Figure 4 with the help of a red dot for dead nodes.

All the sensors are communicating over a short distance via a wireless medium to accomplish a common task, for example, environment monitoring, battlefield surveillance, and industrial process control. Wireless sensor networks have following unique constraints and characteristics:

- ***Randomly deployed sensor network***: Sensor nodes are usually randomly deployed in the field of interest.
- ***Battery – operated sensor nodes:*** Sensor nodes are battery operated. In most situations, they are deployed in a harsh or hostile environment, where it is very difficult or even impossible to change or recharge the batteries.
- ***Resource constraints:*** Sensor nodes are highly limited in resources, i.e. energy, computation, and storage capacities.
- Autonomous ***configuration:*** Usually the sensor nodes are randomly deployed without any careful planning and measurements. Once deployed, sensor nodes have to be configuring themselves autonomously into a communication network.
- ***Application specific:*** A sensor network is designed and deployed usually for a specific application. The design requirements of sensor networks are changed according to its application.

- ***Unreliable sensor nodes:*** The sensor nodes are usually deployed into harsh and hostile environments where they are operated without any attendance. There are always chances to physical damages or failures with the sensor nodes.
- ***Unstable dynamic topology:*** Topology of wireless sensor network is changed frequently due to node failure, node damage, new node addition, energy depletion, or channel fading etc.
- ***No global*** addressing scheme***:*** Due to the large number of sensor nodes, it is usually impossible to build a global addressing scheme for a sensor network because it would introduce a high overhead for the identification maintenance;
- ***Many - to - one traffic pattern****:* In most of the sensor networks, the data sensed by all the sensor nodes will flow from multiple sensor nodes to a particular base station to follow many-to-one traffic pattern.
- ***Data Redundancy:*** In most of the sensor networks, data sensed by multiple sensors in a region is redundant.

2. SECURITY REQUIREMENTS IN WSNs

There are two basic goal of security in WSNs, i.e. **Information Security** to protect the critical data and information stored in the memory of sensor nodes such as confidential decryption keys and **Network Security** to keep track the information at the time of communication when the sensed data is travelling from sensor to the base station. The security requirements in WSNs include:

- ***Availability:*** Which ensures that the desired network services are available and accessible whenever required.
- ***Authorization:*** Which ensures that only authorized sensors can be involved in providing information to the base station.
- ***Authentication***: Which suggest that verify the identity of the participants in a communication and ensure that a message is from the claimed source.
- ***Confidentiality***: Which ensures that the classified data will not be revealed to anyone other than the desired recipients.
- ***Integrity***: Which ensures that the received message was not modified during the transmission by some intermediate malicious node.

- ***Non-repudiation:*** which ensures that a node cannot deny sending a message it has previously sent.
- ***Freshness***: Which ensures that the data is recent and ensures that no adversary can replay old messages.
- ***Forward secrecy:*** This ensures that a sensor should not be able to read any future messages after it leaves the network.
- ***Backward secrecy:*** This ensures that a joining sensor should not be able to read any previously transmitted message.
- ***Location awareness:*** This ensures that the damage cannot be spread from the victimized area to the entire network by security attack even if the sensor node is compromised.

The security requirements in WSNs are usually achieved with the help of around cryptography. However, due to the constraints in WSNs, many already existing secure algorithms are not practical for use.

3. LITERATURE REVIEW

Recently, many schemes were proposed to secure the communication in WSNs. This section classifies WSNs security based on the application scenarios, including cryptography, integrity, authentication and key management.

A **survey of WSNs security threats** affecting different layers along with their defense mechanism is presented in [1]. Author in the proposed work have survey the major topics in wireless sensor network security architecture framework which includes the requirements in the sensor security, classify many of the current attacks, their corresponding defensive measures and finally the classification of secure routing protocols along with their design issues.

Xi Luo et al. [2] propose three schemes to defend against the **traffic analysis attacks**. Firstly, a random routing scheme is proposed to provide path diversity. Secondly, combine RRS with a dummy packet injection scheme to confuse the adversary by tracing or tracing back the forwarded packet to reach the receiver or source. Finally, an anonymous communication scheme is proposed to hide the identities of all nodes that participate in packets transmission. Simulation result confirm the proposed scheme can

efficiently defend against traffic analysis attacks, take less delivery time and achieve uniform energy consumption.

Tamara Bonaci et al. [3] address the problem of **physical node capture attacks** in wireless sensor networks and provide a control theoretic framework to model physical node capture, cloned node detection and revocation of compromised nodes. By combining probabilistic analysis of logical key graphs and linear control theory, authors derive a dynamical model that efficiently describes network behavior under attack. In the proposed scheme, author has developed a network response strategy, which guarantees secure network connectivity and stability under attack.

Bhoopathy et al. [4] suggested an **energy constrained secure hierarchical data aggregation** in Wireless Sensor Networks. Proposed scheme divided the network into clusters, each cluster begins with an aggregator and aggregator was connected to sink. Based on distance to sensor nodes and its energy level, the aggregator detects the node. Separate keys were distributed to the two levels i.e., sensor node to the aggregator and aggregator to the sink. Whenever a data had to be sent from a sensor node to another node; initially the sensor node encrypts the data using a key and sends it to the aggregator.

Araujo et al. [5] surveyed about the **challenges and open problem** in wireless sensor networks. In the proposed work, author have describe a wide variety of attacks, including communication attack, attack against privacy, node targeted attack, power consumption attack, policy attack and cryptography attack and also proposed different security measures to handle these attacks.

P. Kalyani et al. [6] have proposed a novel method, which uses three algorithms hybrid to achieve the **increase in decryption speed**, which in turn reduces the energy used for computation and enhances its performance compared with the existing authentication using classical RSA algorithm. Simulation results show that the proposed scheme provides better performance when compared to the existing RSA.

S. Prasanna et al. [7] presents an overview of the different applications of the wireless sensor networks and various **security related issues in WSNs**.

Nanrun Zhou et al. [8] proposed an **identity-based key management scheme** for wireless sensor networks, where the node identity is used to encrypt the key generating

material. The pair-wise key is generated by the material ultimately. The security of the proposed scheme is analyzed with the provable security. Simulation results prove that the proposed scheme is more secure against some active attacks such as tampering and impersonation. The storage and communication overheads of the proposed scheme are low enough to fit for wireless sensor networks. Addition and revocation of the nodes with backward-security and forward-security respectively make the scheme more feasible and flexible.

Yuexin Zhang et al. [9] propose an efficient **key pre-distribution scheme** based on two polynomials in wireless mesh networks by employing the nature of heterogeneity. Proposed scheme realizes the property of bloom filters, i.e., neighbor nodes can discover their shared keys but have no knowledge on the different keys possessed by the other node, without the probability of false positive. The analysis presented in the research shows that the proposed scheme has the ability to establish three different security level keys and achieves the property of self adaptive security for sensor networks with acceptable computation and communication consumption.

Manjusha Pandey et al. [10] have presented **anti-traffic analysis privacy preservation** in WSN. The proposed scheme is energy efficient which can also preserve the privacy of location information of base station and the source nodes so that the adversary cannot take down these nodes.

Xiong et al. [11] proposed a fast and Lightweight **pairing-based cryptographic** library for Wireless Sensor Networks. The library has an additional of one identity-based encryption scheme and two short signature schemes. The proposed scheme contains several new algorithms and techniques showing an improvement in speed while reducing the memory usage of the library.

Wander et al. [12] presents a **comparison of public-key algorithms**, RSA and elliptic curve cryptography. According to the proposed scheme, the requirement for energy efficiency suggests that in most cases communication is expensive than computation. Simulation results prove that more computationally intensive algorithms cannot be used to incorporate security due to energy considerations.

Q-composite key scheme [13], generalization of [12], improves the resilience of the network (for the same amount of key storage) and requires an attacker to compromise many more nodes in order to negotiate extra communication links.

In [14] a **Key-Management Scheme** for distributed sensor networks is presented. In proposed scheme the selective distribution, revocation and node re-keying methods are employed without any substantial computation and communication overheads to satisfy both operational and security requirements in distributed wireless network.

Blom et al. [15] proposed a **key pre-distribution scheme** that allows any two nodes of a group to find a pair-wise key. The security parameter of the scheme is secure as long as no more than the fix number of nodes are compromised, and the network is perfectly secure.

Huang et al. [16] have proposed a **secure encrypted-data aggregation scheme** for mobile wireless sensor networks. The proposed scheme for data aggregation removes redundant sensor readings without using any encryption algorithm while maintaining data privacy during transmission. However, the presented scheme lacks in terms of integrity.

Secure hierarchical in-network data aggregation proposed by Chan et al. [17] guarantees the adversary can never gain any advantage from misrepresenting intermediate aggregation computations. The main algorithm forces the adversary to commit to its choice of intermediate aggregation results using a SUM aggregation after that each sensor node independently verifies their contributions towards aggregation.

4. RESEARCH OBJECTIVE

There is a tradeoff between security, reliability, availability, and energy efficiency in WSN. This motivates us to design a secure framework for WSNs. The objectives include:

- To achieve performance efficiency and reduce resource requirements, an encryption mechanism is proposed to be used in which a message is segmented into parts and each part will participate in encrypting the message. Proposed technique will eliminate the requirement of key distribution and establishment.
- A secret key establishment between the source and destination by multiple communication paths can decrease the risk of path key exposure problem. Therefore, multi-path key establishment solutions are resilient to resist stop forwarding, ensure

network availability from connective failure and prevent compromised sensors from knowing the secret in WSNs.

- There is need to develop an efficient and secure data aggregation technique essential for cluster based WSNs for eliminating data redundancy to reduce energy consumption and hence to extend lifetime of the entire network.
- There is need to design an efficient security mechanism to detect malicious nodes. The basic idea of detection of malicious behavior node is to provide. A hop-by-hop authentication based on intelligent biologically inspired sensor nodes is proposed for detecting malicious nodes in WSNs.

5. WORK TO BE CARRIED OUT

Security is very important research objective in the field of wireless sensor networks. There are still many goals and open problems in the field of WSNs security. The need for security will grow significantly with the rapid use of WSNs. Existing solutions are not suitable for resource constrained devices, so new techniques are required to make them secure. A simple model will be required that would enable fully functional security in WSNs. A brief summary of the work to be carried out the field of WSNs security is given below:

- To analyze security issue in wireless sensor networks.
- To investigate the application of Cryptography in wireless sensor networks.
- To design an efficient key management scheme that will solve many of the shortcomings of existing protocols in the wireless sensor networks.
- To design secure data aggregation mechanisms for wireless sensor networks.
- To develop a model for removing & replacement of compromised Sensor Nodes from Wireless Sensor Networks.
- To develop a model to achieve the principle of forward secrecy, i.e. a sensor should not be able to read any future data.
- To develop a model to achieve the principle of backward secrecy, i.e. a joining sensor should not be able to read any past data.

The proposed work will consider the above challenges in the research work. The challenges include data encryption, secure data aggregation scheme, secure key

management, malicious node detection, and node revocation and replacement scheme.

REFERENCES

[1] . Md Abdul Azeem and Dr. Khaleel-ur-Rahman khan, A. V. Pramod, "Security Architecture Framework and Secure Routing Protocols in Wireless Sensor Networks-Survey", in International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011.

[2] . X Luo, Xu Ji and Myong-Soon Park, "Location privacy against traffic analysis attacks in wireless sensor networks", in International Conference on Information Science and Applications (ICISA), Vol. 1. Seoul, Korea, pp. 1–6, April 2010.

[3] . Tamara Bonaci, Linda Bushnell and Radha Poovendran, "Node capture attacks in wireless sensor networks: a system theoretic approach", in 49th IEEE Conference on Decision and Control (CDC), Vol. 1. Atlanta, Georgia, USA, pp. 6765–6772, December 2010.

[4] . Bhoopathy, V. and R.M.S. Parvathi, "Energy Constrained Secure Hierarchical Data Aggregation in Wireless Sensor Networks", in American Journal of Applied Sciences, ISSN 1546-9239, Vol.9, No.6, pp. 858-864, 2012.

[5] . Alvaro Araujo, Javier Blesa, Elena Romero and Daniel Villanueva, "Security in cognitive wireless sensor networks - Challenges and open problems", in EURASIP Journal on Wireless Communications and Networking 2012, 2012:48, February 2012.

[6] . Kalyani, P. and C. Chellappan., "Enhanced RSACRT for Energy Efficient Authentication to Wireless Sensor Networks Security", American Journal of Applied Sciences 9 (10): 1660-1667, ISSN 1546-9239, 2012.

[7] . S.Prasanna and Srinivasa Rao , "An Overview of Wireless Sensor Networks Applications and Security", in International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Vol. 2, Issue-2, May 2012.

[8] . Nanrun Zhou, Qiongxi Jiang and Xun Chen, "Identity-based Key Management Scheme with Provable Security for Wireless Sensor Networks", in Journal of Information & Computational Science Vol. 8, No. 14, pp. 3075- 3081, 2011.

[9] . Yuexin Zhang, Li Xu and Xinyi Huang, "Polynomial-based Key Pre-distribution Scheme in Wireless Mesh Networks", in Journal of Computational Information Systems, Vol. 8, No. 6, pp. 2539–2549, 2012.

[10] . Manjusha Pandey and Shekhar Verma, "Residual Energy Based Anti-Traffic Analysis Privacy Preservation in WSN", in I. J. Computer Network and Information Security, pp.

21-29, 2012.

[11] . Xiaokang Xiong, Duncan S. Wong and Xiaotie Deng, “TinyPairing: A fast and lightweight pairing-based cryptographic library for wireless sensor networks”, in Proceedings of the 2010 IEEE Wireless Communications and Networking Conference, IEEE explore Press, Sydney, DOI: 10.1109/WCNC.2010.5506580, pp: 1-6, April 18-21, 2010.

[12] . Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta and Sheueling Chang Shantz, “Energy analysis of public-key cryptography for wireless sensor networks” in Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications, 18Xplore Press, DOI: 10.1109/PERCOM-2005, pp: 324-328, March 8-12, 2005.

[13] . Haowen Chan, Adrian Perrig and Dawn Song, “Random key pre distribution schemes for sensor networks”, in IEEE Symposium on Security and Privacy, Berkeley, California, ISSN: 1081-6011, Print ISBN: 0-7695-1940-7, pp. 197–213, 11-14 May 2003.

[14] . Laurent Eschenauer and Virgil D. Gligor, “A key-management scheme for distributed sensor networks”, in Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41–47, November 18–22, 2002.

[15] . Blom, R., “An optimal class of symmetric key generation systems”, in proceedings of EUROCRYPT 84 (Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, Eds.): Advances in Cryptology-EUROCRYPT’84, LNCS 209, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, pp. 335–338, 1985.

[16] . Shih-I Huang and Shiuhpyng Shieh, “SEA: Secure Encrypted Data Aggregation in Mobile Wireless Sensor Networks”, in Proceedings of the International Conference on Computational Intelligence and Security, IEEE Explore Press, Harbin, DOI: 10.1109/CIS.2007.207, pp: 848-852, December 15-19, 2007.

[17] . Chan, H., A. Perrig and D. Song, “Secure hierarchical in-network aggregation in sensor networks”, in Proceedings of the 13th ACM Conference on Computer and Communications Security, ACM, Alexandria, VA, USA, DOI: 10.1145/1180405.1180440, pp: 278-287, Oct. 30-Nov. 03,2006.